On Lee Association Scheme over $mathbb{Z}_4$, Terwilliger algebras and the Assmus-Mattson Theorem (Research on finite groups, algebraic combinatorics and vertex operator algebras)

AUTHOR(S):

Morales, John Vincent S.

CITATION:

Morales, John Vincent S.. On Lee Association Scheme over $mathbb{Z}_4$, Terwilliger algebras and the Assmus-Mattson Theorem (Research on finite groups, algebraic combinatorics and vertex operator algebras). 数理解析研究所講究録 2017, 2053: 68-79

ISSUE DATE:

2017-10

URL:

http://hdl.handle.net/2433/237129

数理解析研究所講究録
第2053巻 2017年 68-79

On Lee Association Scheme over $\mathbb{Z}_4$, Terwilliger algebras and the Assmus-Mattson Theorem*

John Vincent S. Morales†

Abstract

Let C denote a linear code of length n over a finite field $\mathbb{F}_q$ and let $C^{\perp}$ denote the corresponding dual. The Assmus-Mattson theorem states that combinatorial designs can be obtained from the supports of codewords of C with fixed weight type whenever the Hamming weight enumerators of C and $C^{\perp}$ satisfy certain conditions. This famous result has been strengthened and extended to many different settings including the Assmus-Mattson type theorems for $\mathbb{Z}_4$-linear codes due to Tanabe (2003), and due to Shin, Kumar and Helleseth (2004). In this paper, we discuss an Assmus-Mattson type theorem for block codes where the alphabet is the vertex set of some commutative association scheme. This particular theorem generalizes the Assmus-Mattson type theorems mentioned above as well as the original. In proving our results, we invoke several techniques from multivariable polynomial interpolation and from the representation theory of Terwilliger algebras. This is based on a joint work with Hajime Tanaka.

1 Introduction

We begin by recalling the famous *Assmus–Mattson theorem*:

Theorem 1.1 (Assmus and Mattson [1, Theorem 4.2]). *Let C be a linear code of length n over $\mathbb{F}_q$ with minimum weight δ. Let $C^{\perp}$ denote the dual code of C with minimum weight δ^*. Suppose that an integer t $(1 \leqslant t \leqslant n)$ exists such that either there are at most $\delta - t$ weights of $C^{\perp}$ in $\{1, 2, \ldots, n-t\}$ or there are at most $\delta^* - t$ weights of C in $\{1, 2, \ldots, n-t\}$. Then the supports of the words of any fixed weight in C form a t-design (possibly with repeated blocks).*

The theorem mentioned above has been proven and strengthened in many different settings (see [11, 10, 32, 2, 36, 23, 38] for instance). The objective of this paper is to present a theorem which unifies many of the known generalizations and extensions of Theorem 1.1. We advise the reader to check [29] for a more detailed discussion of the

*presented at the Research on Finite Groups, Algebraic Combinatorics and Vertex Operator Algebras held in RIMS at Kyoto University, Kyoto, Japan on 6 December 2016

†Graduate School of Information Sciences, Tohoku University, Sendai, Japan
email: moralesjohnvince@ims.is.tohoku.ac.jp

topic.

Recent interests in constructing combinatorial designs from codes began when Gulliver and Harada [17] and Harada [18] found new 5-designs from the lifted Golay code of length 24 over $\mathbb{Z}_4$ (among others) through computer search. Later, these constructions were further explained and generalized by Bonnecaze, Rains, and Solé [6]. Motivated by these results, Tanabe [35] then obtained an Assmus–Mattson-like theorem for linear codes over $\mathbb{Z}_4$ with respect to the symmetrized weight enumerator. Though Tanabe's theorem can find 5-designs from the lifted Golay code over $\mathbb{Z}_4$, the technique involves finding the ranks of matrices having quite complicated entries. As a consequence, verifying the conditions by manual computations is difficult. Tanabe [37] then presented a simpler version of his theorem, and we can easily check its conditions by hand for the lifted Golay code over $\mathbb{Z}_4$.

By an *Assmus–Mattson-type* theorem, we mean a theorem which enables us to find combinatorial t-designs by just looking at some kind of weight enumerator of a code (and some other information such as linearity). It should be noted that the combinatorial designs obtained from such as a theorem does not necessarily give the best estimate for the integer t but the wide range of applicability is commendable.

We shall see that there corresponds a weight enumerator for every s-class translation association scheme. In particular, the Hamming weight enumerator is related to the *Hamming association schemes* which are extensions of 1-class association schemes. Hamming schemes belong to a family called metric and cometric association schemes, and Tanaka [38] showed that Theorem 1.1 can be interpreted and generalized from this point of view. On the other hand, the situation becomes more complicated when $s > 1$ as we are considering an extension of a finer translation association scheme.

In this paper, we present an Assmus–Mattson-type theorem for codes over the vertex set of some s-class translation scheme. In general, the weights of a codeword take the form $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_s)$ where each α_i is a nonnegative integer and $\alpha_1 + \cdots + \alpha_n \leqslant n$. We count the *number* of weights in a given interval when $s = 1$ as in Theorem 1.1, but in case $s > 1$ then we speak of the *minimal degree* of subspaces of the polynomial ring $\mathbb{R}[\xi_1, \xi_2, \ldots, \xi_s]$ which allow unique Lagrange interpolation with respect to those weights (which are lattice points in $\mathbb{R}^s$) contained in a given region. When specialized to the case of $\mathbb{Z}_4$-linear codes with the symmetrized weight enumerator as in [35, 37], the association scheme on the alphabet $\mathbb{Z}_4$ has two classes R_1 and R_2, together with the identity class R_0, defined by

$$(x, y) \in R_i \iff y - x = \pm i \ (\mathrm{mod} 4) \quad (x, y \in \mathbb{Z}_4)$$

for $i \in \{0, 1, 2\}$, and the extension of this 2-class association scheme is called the *Lee association scheme* over $\mathbb{Z}_4$. Our results give a slight extension of Tanabe's theorem in [37]. Moreover, the Assmus–Mattson-type theorem for $\mathbb{Z}_4$-linear codes with the Hamming weight enumerator due to Shin, Kumar, and Helleseth [31] can also be recovered. In proving our results, we make heavy use of the representation theory of the *Terwilliger algebra* [41, 42, 43], which is a non-commutative semisimple matrix $\mathbb{C}$-algebra with respect to a fixed vertex of an association scheme.

2 Preliminaries

In this section we briefly review some basic concepts concerning commutative association schemes and related algebras. We advise the reader to check [4, 9, 25] for a more thorough discussion of the topic.

Let X be a nonempty finite set. Let V denote the vector space over $\mathbb{C}$ of column vectors with coordinates indexed by X. Define the vector $\widehat{x} \in V$ for each $x \in X$ such that y-coordinate of $\widehat{x}$ is δ_{xy} for all $y \in X$ where δ is the Kronecker delta function. The set $\{\widehat{x} \mid x \in X\}$ forms an orthonormal basis for V with respect to the Hermitian inner product $\langle u, v\rangle = u^t\bar{v}$ for all $u, v \in V$. Let $\mathrm{Mat}_X(\mathbb{C})$ denote the $\mathbb{C}$-algebra of all matrices over $\mathbb{C}$ with rows and columns indexed by X. Observe that $\mathrm{Mat}_X(\mathbb{C})$ acts on V by left multiplication. Let $\mathcal{R} = \{R_0, R_1, \ldots, R_s\}$ denote a partition on $X \times X$ and let $A_i \in \mathrm{Mat}_X(\mathbb{C})$ denote the characteristic matrix of $R_i \subseteq X \times X$. The pair $(X, \mathcal{R})$ is called a *commutative association scheme* on s classes if

(i) $A_0 = I$, the identity matrix;

(ii) $\sum_{i=0}^{s} A_i = J$, the all ones matrix;

(iii) $\{A_0, A_1, \ldots, A_s\}$ is closed under conjugate-tranpose;

(iv) $A_iA_j = A_jA_i \in M := \sum_{k=0}^{s} \mathbb{C}A_k$ for $0 \leqslant i, j \leqslant s$.

In this case, we call X the *vertex set* and $\mathcal{R} = \{R_0, \ldots, R_s\}$ the set of *associate classes*. We call V the *standard module* for the commutative association scheme $(X, \mathcal{R})$.

The *Bose-Mesner algebra* M is the commutative subalgebra of $\mathrm{Mat}_X(\mathbb{C})$ with basis consisting of the *associate matrices* $A_0, A_1, \ldots, A_s$. There exists a second basis for M consisting of the matrices $E_0 = |X|^{-1}J, E_1, \ldots, E_s$ such that $E_0 + E_1 + \cdots + E_s = I$ and $E_iE_j = \delta_{ij}E_i$ for all $0 \leq i, j \leq s$. The matrices $E_0, E_1, \ldots, E_s$ are called *primitive idempotents*. We define the change-of-basis matrices P and Q by

$$A_i = \sum_{j=0}^{s} P_{ji}E_j, \tag{1}$$

$$E_i = |X|^{-1} \sum_{j=0}^{s} Q_{ji}A_j. \tag{2}$$

we refer to P and Q as the *first* and *second eigenmatrix* of $(X, \mathcal{R})$, respectively.

Fix $x \in X$. We recall the *dual Bose-Mesner algebra $M^*(x)$ with respect to x*. Define diagonal matrices $E_i^* = E_i^*(x)$ and $A_i^* = A_i^*(x)$ in $\mathrm{Mat}_X(\mathbb{C})$ for each integer $0 \leq i \leq s$ such that the (y, y)-entries are given by $(E_i^*)_{yy} = (A_i)_{xy}$ and $(A_i^*)_{yy} = |X|(E_i)_{xy}$ for each $y \in X$. Then $M^*(x)$ is the commutative subalgebra of $\mathrm{Mat}_X(\mathbb{C})$ that has two special bases, $\{E_0^*, E_1^*, \ldots, E_s^*\}$ and $\{A_0^*, A_1^*, \ldots, A_s^*\}$. The matrices $E_0^*, E_1^*, \ldots, E_s^*$ are called *dual primitive idempotents with respect to x* and the matrices $A_0^*, A_1^*, \ldots, A_s^*$ are called *dual associate matrices with respect to x*.

Let $T(x)$ denote the subalgebra of $\mathrm{Mat}_X(\mathbb{C})$ that is generated by M and $M^*(x)$. We call $T(x)$ the *Terwilliger algebra* of (X, R) with respect to x. Note that $T(x)$ is

finite-dimensional and is semisimple since $T(x)$ is closed under the conjugate transpose map. On the standard module V, any two non-isomorphic irreducible modules for $T(x)$ are orthogonal. For every irreducible $T(x)$-module $W \subseteq V$, define the sets

$$W_s = \{0 \leq i \leq s \mid E_i^* W \neq 0\} \text{ and } W_s^* = \{0 \leq i \leq s \mid E_i W \neq 0\}.$$

We call W_s, W_s^* the *support* and *dual support* of W, respectively. We say W is *thin* (resp. *dual thin*) if $\dim(E_i^* W) \leq 1$ for all i (resp. $\dim(E_j W) \leq 1$ for all j). There exists a unique irreducible module for $T(x)$ that is both thin and dual thin for which the support and the dual support are both equal to $\{0, 1, \ldots, s\}$. We call this the *primary module for* $T(x)$.

We end this section with a connection between commutative association schemes and codes. The reader may refer to [12, 13] for more details. For the rest of this section, let C denote a subset of X and let $\widehat{C}$ denote the characteristic vector of $C \subseteq X$. In this paper, we shall call C a *code* if $1 < |C| < |X|$. Assume for a moment that C is a code. The *inner distribution* of C is the vector $a = (a_0, a_1, \ldots, a_s) \in \mathbb{R}^{s+1}$ where the scalars a_i are defined by

$$a_i = |C|^{-1} \langle \widehat{C}, A_i \widehat{C} \rangle = |C|^{-1} \cdot |R_i \cap (C \times C)|.$$

Clearly, the scalars a_i are nonnegative. Observe that using (2), we obtain

$$\langle \widehat{C}, E_i \widehat{C} \rangle = |X|^{-1} |C| (aQ)_i$$

for every i $(0 \leq i \leq s)$ where $(aQ)_i$ denotes the ith coordinate of the vector $aQ \in \mathbb{R}^{s+1}$. The vector aQ is often referred to as the *MacWilliams transform* of a.

3 Translation Schemes and Extensions

Let $(X, \mathcal{R})$ denote a commutative association scheme with s classes. Assume further that X has the structure of an abelian group (written additively) with identity 0. We call $(X, \mathcal{R})$ a *translation association scheme* if for every $0 \leq i \leq s$ and for every $z \in X$ we have $(x, y) \in R_i$ implies $(x + z, y + z) \in R_i$. For the rest of the section, assume that $(X, \mathcal{R})$ is a translation association scheme and we shall pick the identity element as the base vertex when dealing with Terwilliger algebras of translation association schemes. We show that there exists an association scheme $(X^*, \mathcal{R}^*)$ that is dual to $(X, \mathcal{R})$. It turns out that this dual is also a translation association scheme.

Let X^* denote the character group of X with identity element ι. To each $\varepsilon \in X^*$ we associate the vector

$$\widehat{\varepsilon} = |X|^{-1/2} \sum_{x \in X} \overline{\varepsilon(x)}\, \widehat{x} \in V.$$

By the orthogonal relations of the characters, we observe that the set $\{\widehat{\varepsilon} \mid \varepsilon \in X^*\}$ forms an orthonormal basis of V. We claim that these basis vectors are eigenvectors for the associate matrices $A_0, A_1, \ldots, A_s$. In particular, one routinely obtains

$$\langle A_i \widehat{\varepsilon}, \widehat{\tau} \rangle = \begin{cases} 0 & \text{if } \varepsilon \neq \tau \\ \sum_{x \in X_i} \overline{\varepsilon(x)} & \text{if } \varepsilon = \tau \end{cases}$$

for every $\varepsilon, \tau \in X^*$ where $X_i = \{x \in X \mid (0,x) \in R_i\}$ for each $0 \leq i \leq s$. Consequently, each vector $\widehat{\varepsilon}$ is contained in one of the subspaces E_iV of V. Thus, we have a partition

$$X^* = X_0^* \sqcup X_1^* \sqcup \cdots \sqcup X_s^*,$$

given by $X_i^* = \{\varepsilon \in X^* : \hat{\varepsilon} \in E_iV\}$ $(0 \leqslant i \leqslant s)$. Define the set $\mathcal{R}^* = \{R_0^*, R_1^*, \ldots, R_s^*\}$ of nonempty binary relations on X^* by

$$R_i^* = \{(\varepsilon, \eta) \in X^* \times X^* : \eta\varepsilon^{-1} \in X_i^*\} \quad (0 \leqslant i \leqslant s).$$

It turns out that the pair $(X^*, \mathcal{R}^*)$ is again a translation association scheme called the *dual* of $(X, \mathcal{R})$. Suppose that P^* and Q^* are the first and second eigenmatrices of $(X^*, \mathcal{R}^*)$, respectively. Then $P^* = Q$ and $Q^* = P$, and that

$$P_{ji} = \sum_{x \in X_i} \overline{\varepsilon(x)} \quad (\varepsilon \in X_j^*), \qquad Q_{ji} = \sum_{\varepsilon \in X_i^*} \varepsilon(x) \quad (x \in X_j).$$

We view V together with the basis $\{\widehat{\varepsilon} : \varepsilon \in X^*\}$ as the standard module for $(X^*, \mathcal{R}^*)$.

We call a code C in X an *additive code* if C is a subgroup of X. Assume for the moment that C is an additive code, and let the vector $a = (a_0, a_1, \ldots, a_s)$ denote its inner distribution. We claim that $a_i = |X_i \cap C|$ for each $0 \leq i \leq s$. This follows from the fact that every element $z \in X_i \cap C$ can be expressed as $y - x$ where $x, y \in C$ in exactly $|C|$ ways. In this case, the vector a is also called the *weight distribution* of C. The *dual code* of C is the subgroup $C^\perp$ in X^* defined by

$$C^\perp = \{\varepsilon \in X^* : \varepsilon(x) = 1 \text{ for all } x \in C\}.$$

It turns out that $|X_i^* \cap C^\perp| = |C|^{-1}(aQ)_i$ $(0 \leq i \leq s)$ so that $|C|^{-1}(aQ)$ gives the weight distribution of $C^\perp$.

The group operation on X^* is multiplicative. In many cases we may view a code in X^* as a code in X by fixing a (non-canonical) isomorphism $X \to X^*$ $(x \mapsto \varepsilon_x)$ such that

$$\varepsilon_x(y) = \varepsilon_y(x) \quad (x, y \in X). \tag{3}$$

Thus, the dual code of an additive code in X becomes again an *additive* code in X. For more details about translation association schemes, the reader may refer to [12, Chapter 6], [9, §2.10], and [25, §6].

For the rest of this paper, we will fix an integer $n \geq 2$. Delsarte [12, §2.5] gave a construction of a new commutative association scheme from $(X, \mathcal{R})$ with vertex set X^n as follows. For a sequence $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_s) \in \mathbb{N}^s$, let $|\alpha| = \sum_{i=1}^s \alpha_i$. For any two vertices $\boldsymbol{x} = (x_1, x_2, \ldots, x_n), \boldsymbol{y} = (y_1, y_2, \ldots, y_n) \in X^n$, define the *composition* of $\boldsymbol{x}, \boldsymbol{y}$ to be the vector $c(\boldsymbol{x}, \boldsymbol{y}) = (c_1, c_2, \ldots, c_s) \in \mathbb{N}^s$ where

$$c_i = |\{\ell : (x_\ell, y_\ell) \in R_i\}| \quad (1 \leqslant i \leqslant s).$$

Let S denote the set of all possible compositions. For every $\alpha \in S$, define the binary relation $\boldsymbol{R}_\alpha$ on X^n by

$$\boldsymbol{R}_\alpha = \{(\boldsymbol{x}, \boldsymbol{y}) \in X^n \times X^n : c(\boldsymbol{x}, \boldsymbol{y}) = \alpha\}.$$

Then it follows that the pair $(X^n, \{\boldsymbol{R}_\alpha : \alpha \in S\})$ is a commutative association scheme called the *extension* of $(X, \mathcal{R})$ of length n. We shall identify its standard module with $V^{\otimes n}$ so that $\widehat{\boldsymbol{x}} := \widehat{x}_1 \otimes \widehat{x}_2 \otimes \cdots \otimes \widehat{x}_n$ for every $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in X^n$. For every $\alpha \in S$, the associate matrix $\boldsymbol{A}_\alpha$ is the characteristic matrix of $\boldsymbol{R}_\alpha \subseteq X^n$ and is then given by

$$\boldsymbol{A}_\alpha = \sum_{i_1, i_2, \ldots, i_n} A_{i_1} \otimes A_{i_2} \otimes \cdots \otimes A_{i_n}, \tag{4}$$

where the sum is over $i_1, i_2, \ldots, i_n \in \mathbb{N}$ such that

$$\{i_1, i_2, \ldots, i_n\} = \{0^{n-|\alpha|}, 1^{\alpha_1}, 2^{\alpha_2}, \ldots, s^{\alpha_s}\}$$

as multisets. In particular, the Bose-Mesner algebra $\boldsymbol{M}$ of $(X^n, \{\boldsymbol{R}_\alpha : \alpha \in S\})$ coincides with the n^{th} symmetric tensor space of M. Similar expressions hold for the primitive idempotents, dual idempotents, and the dual associate matrices of $(X^n, \{\boldsymbol{R}_\alpha : \alpha \in S\})$, denoted by the $\boldsymbol{E}_\alpha, \boldsymbol{E}^*_\alpha$, and the $\boldsymbol{A}^*_\alpha$, respectively. Recall that if x_0 is the identity element in X then the vertex $\boldsymbol{x}_0 := (x_0, x_0, \ldots, x_0)$ is the identity element in X^n and is then chosen as the base vertex. We denote the corresponding dual Bose-Mesner algebra and the Terwilliger algebra by $\boldsymbol{M}^*$ and $\boldsymbol{T}$, respectively. We also consider the partition

$$X^n = \bigsqcup_{\alpha \in S} (X^n)_\alpha$$

where $(X^n)_\alpha = \{\boldsymbol{x} \in X^n : (\boldsymbol{x}_0, \boldsymbol{x}) \in \boldsymbol{R}_\alpha\}$.

Let $\{\boldsymbol{e}_i : 1 \leqslant i \leqslant s\}$ be the standard basis of $\mathbb{R}^s$. It can be routinely checked that

$$\boldsymbol{A}_{\boldsymbol{e}_i} = \sum_{\substack{\alpha \in \mathbb{N}^s \\ |\alpha| \leqslant n}} \left(\sum_{j=0}^{s} \alpha_j P_{ji} \right) \boldsymbol{E}_\alpha, \quad \boldsymbol{A}^*_{\boldsymbol{e}_i} = \sum_{\substack{\alpha \in \mathbb{N}^s \\ |\alpha| \leqslant n}} \left(\sum_{j=0}^{s} \alpha_j Q_{ji} \right) \boldsymbol{E}^*_\alpha, \tag{5}$$

where $\alpha_0 := n - |\alpha|$. More generally, Mizukawa and Tanaka [27] described the eigenmatrices of $(X^n, \{\boldsymbol{R}_\alpha : \alpha \in S\})$ in terms of certain s-variable hypergeometric orthogonal polynomials that generalize the Krawtchouk polynomials. The reader may also refer to [22] and [21].

Suppose $(X, \mathcal{R})$ is a translation association scheme and let $(X^n, \{\boldsymbol{R}_\alpha : \alpha \in S\})$ is the extension of length n of the association scheme (X, R). To this end, we define a corresponding weight enumerator of C for every additive code C in X^n and we recall a generalization of the well-known *MacWilliams identity*. Let $\xi = (\xi_0, \xi_1, \ldots, \xi_s)$ be a sequence so that $\xi_0, \xi_1, \ldots, \xi_s$ are indeterminates. For every element $\alpha \in S$, we define

$$\xi^\alpha = \xi_0^{n-|\alpha|} \xi_1^{\alpha_1} \xi_2^{\alpha_2} \cdots \xi_s^{\alpha_s}.$$

Now, we consider a code C in X^n with corresponding inner distribution $a = (a_\alpha)_{\alpha \in S}$. Define the polynomial $w_C(\xi)$ in $\mathbb{R}[\xi] = \mathbb{R}[\xi_0, \xi_1, \ldots, \xi_s]$ given by

$$w_C(\xi) = \sum_{\alpha \in S} a_\alpha \xi^\alpha.$$

Since $(X^n, \{\boldsymbol{R}_\alpha : \alpha \in S\})$ is a translation association scheme, the vector a is also the weight distribution of C. We refer to the polynomial $w_C(\xi)$ as the *weight enumerator*

of C. It should be remarked that $(X^n, \{\boldsymbol{R}_\alpha : \alpha \in S\})$ and $(X^{*n}, \{\boldsymbol{R}^*_\alpha : \alpha \in S^*\})$ are dual to each other. It can be shown that

$$w_{C^\perp}(\xi) = |C|^{-1} w_C(\xi Q^{\mathsf{T}}).$$

This generalizes the well-known *MacWilliams identity*. This equation implies that the weight enumerator of the dual code $C^\perp$ can be easily obtained from the weight enumerator of the code C.

4 Codes over $\mathbb{Z}_4$

In this section, we consider abelian group $X = \mathbb{Z}_4$ as the vertex set and discuss different examples of translation association schemes $(X, \mathcal{R})$. We also construct the extension $(X^n, \{\boldsymbol{R}_\alpha : \alpha \in S\})$ of length n of the translation scheme $(X, \mathcal{R})$ and describe the corresponding weight enumerator of an additive code C in X^n.

For our first example, we consider the partition $\mathcal{R} = \{R_0, (X \times X) \backslash R_0\}$ so that $(X^n, \{\boldsymbol{R}_\alpha : \alpha \in S\})$ is an extension of a one-class association scheme. The association scheme $(X^n, \{\boldsymbol{R}_\alpha : \alpha \in S\})$ is called the *Hamming association scheme*. The Hamming schemes are well-studied association schemes and they belong to a family of *metric* and *cometric* schemes. In this case, the corresponding weight enumerator of any additive code in X^n is called the *Hamming weight enumerator*.

For our second example, we consider the partition $\mathcal{R} = \{R_0, R_1, R_2\}$ of $X \times X$ such that $R_i = \{(x, y) \in X \times X \mid y - x = \pm i \pmod 4\}$ for each $0 \leq i \leq 2$. Observe that the pair $(X, \mathcal{R})$ is a two-class translation association scheme. We refer to the extension $(X^n, \{\boldsymbol{R}_\alpha : \alpha \in S\})$ as a *Lee association scheme* over $\mathbb{Z}_4$. The Terwilliger algebras of Lee association schemes over $\mathbb{Z}_4$ are described in [28]. Now let C denote an additive code in X^n and let $w_C(\xi)$ denote the corresponding weight enumerator of C. We refer to $w_C(\xi)$ as the *symmetrized weight enumerator* of C.

Finally, we consider the partition $\mathcal{R} = \{R_0, R_1, R_2, R_3\}$ of $X \times X$ given by

$$\begin{aligned} R_1 &= \{(0,1), (1,2), (2,3), (3,0)\}, \\ R_2 &= \{(0,2), (1,3), (2,0), (3,1)\}, \\ R_3 &= \{(0,3), (1,0), (2,1), (3,2)\} \end{aligned}$$

so that $(X^n, \{\boldsymbol{R}_\alpha : \alpha \in S\})$ is an extension of a three-class association scheme. In this case, the corresponding weight enumerator of any additive code in X^n is called the *complete weight enumerator*.

5 Main Results

In this section, we present the main theorem (Theorem 5.3) as well as some supplements that improve the main theorem (see [29] for the proofs). To do this, we need to recall some concepts from polynomial interpolation (see [14] for more details).

Let F be a finite set of points in $\mathbb{R}^s$. We call a linear subspace $\mathscr{L}$ of $\mathbb{R}[\xi_1, \xi_2, \ldots, \xi_s]$ an *interpolation space* with respect to F if for every $f \in \mathbb{R}[\xi_1, \xi_2, \ldots, \xi_s]$, there exists a unique $g \in \mathscr{L}$ such that $f(z) = g(z)$ for every point $z \in F$. If, in addition, this g always satisfies $\deg f \geqslant \deg g$, then we refer to $\mathscr{L}$ as a *minimal degree* interpolation space. Let $\mathscr{M}(F)$ denote a minimal degree interpolation space with respect to F and define

$$\mu(F) = \max\{\deg f : f \in \mathscr{M}(F)\}.$$

We recall a construction of a minimal degree interpolation space $\mathscr{M}(F)$ due to de Boor and Ron (see [7, 8]). For every non-zero element $f = \sum_{i=0}^{\infty} f_i$ in the ring of formal power series $\mathbb{R}[[\xi_1, \xi_2, \ldots, \xi_s]]$ where f_i is homogeneous of degree i, define

$$f_{\downarrow} = f_{i_0},$$

where $i_0 = \min\{i : f_i \neq 0\}$. Conventionally, we set $0_{\downarrow} := 0$. The theorem below gives us a construction for a minimal degree interpolation space $\mathscr{M}(F)$.

Theorem 5.1 ([7, 8]). *Let F be a finite set of points in $\mathbb{R}^s$. Let $\mathscr{E}$ be the subspace of $\mathbb{R}[[\xi_1, \xi_2, \ldots, \xi_s]]$ spanned by the exponential functions*

$$\exp\left(\sum_{i=1}^{s} z_i \xi_i\right) \quad ((z_1, z_2, \ldots, z_s) \in F).$$

Then the subspace

$$\sum_{f \in \mathscr{E}} \mathbb{R} f_{\downarrow} \subset \mathbb{R}[\xi_1, \xi_2, \ldots, \xi_s]$$

is a minimal degree interpolation space with respect to F.

Theorem 5.1 immediately leads to the following formula for $\mu(F)$ which is well suited for computer calculations:

Supplement 5.2. *For every finite set F of points in $\mathbb{R}^s$, the scalar $\mu(F)$ equals the smallest $m \in \mathbb{N}$ for which the polynomials*

$$\sum_{k=0}^{m} \left(\sum_{i=1}^{s} z_i \xi_i\right)^k \quad ((z_1, z_2, \ldots, z_s) \in F)$$

are linearly independent.

We see that $\mathscr{M}(F)$ exists but is not unique. However, it can be shown that $\mu(F)$ is well-defined that is, it is independent of the choice of $\mathscr{M}(F)$.

We retain the notation of Section 3. For every $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in X^n$, define

$$\operatorname{supp}(\boldsymbol{x}) = \{\ell : x_\ell \neq x_0\} \subset \{1, 2, \ldots, n\}.$$

We call $\operatorname{supp}(\boldsymbol{x})$ the *support* of $\boldsymbol{x}$ (with respect to $\boldsymbol{x}_0$). We now present our main theorem.

Theorem 5.3. *Let C denote a code in X^n and let $w_C(\xi) = \sum_{\alpha\in S} a_\alpha \xi^\alpha$ denote its corresponding weight enumerator. Let $w_{C^\perp}(\xi) = \sum_{\alpha\in S} a^*_\alpha \xi^\alpha$ denote the weight enumerator of the dual code $C^\perp$ of C. Let*

$$F_r = \{\alpha \in S : r \leqslant |\alpha| \leqslant n - r,\ a_\alpha \neq 0\} \quad (1 \leqslant r \leqslant \lfloor n/2 \rfloor),$$

and let

$$\delta^* = \min\{|\alpha| \neq 0 : \alpha \in S \text{ and } a^*_\alpha \neq 0\}.$$

Suppose that an integer t $(1 \leqslant t \leqslant n)$ is such that

$$\mu(F_r) < \delta^* - r \quad (1 \leqslant r \leqslant t). \tag{6}$$

Then the multiset

$$\{\mathrm{supp}(\boldsymbol{x}) : \boldsymbol{x} \in (X^n)_\alpha \cap C\} \tag{7}$$

is a t-design for every $\alpha \in \mathbb{N}^s$ with $|\alpha| \leqslant n$.

We use Theorem 5.3 together with the following "supplements" and these supplements improve the main theorem.

Supplement 5.4. *Let C be a code in X^n. Assume that we are given in advance a set $K \subset S$ such that the multiset (7) is a t-design for every $\alpha \in K$. Then the condition (6) in Theorem 5.3 may be replaced by*

$$\mu(F_r \backslash K) < \delta^* - r \quad (1 \leqslant r \leqslant t).$$

We call a subset C of X^n a *weakly t-balanced array*[1] over $(X, \mathcal{R})$ (with respect to the base vertex $\boldsymbol{x}_0$) if, for any $\Lambda \subset \{1, 2, \ldots, n\}$ and $\gamma \in S$ such that $|\gamma| \leqslant |\Lambda| \leqslant t$, the number

$$\left|\{\boldsymbol{x} \in C : (x_i)_{i\in\Lambda} \in (X^{|\Lambda|})_\gamma\}\right|$$

depends only on $|\Lambda|$ and γ.

Supplement 5.5. *Suppose that $(X, \mathcal{R})$ is a translation association scheme, and that C is an additive code in X^n. Assume that we are given in advance a set $L \subset S$ such that, for every $\alpha \in L$, $(X^{*n})_\alpha \cap C^\perp$ is a weakly t-balanced array over $(X^*, \mathcal{R}^*)$. Then the scalar δ^* in Theorem 5.3 may be replaced by*

$$\min\{|\alpha| : 0 \neq \alpha \in S\backslash L,\ a^*_\alpha \neq 0\}. \tag{8}$$

Supplement 5.6 below was inspired by [37, Theorem 2], and allows us to estimate $\mu(F)$, and hence t, by geometrical considerations. It is a general result about minimal degree interpolation spaces.

Supplement 5.6. *Let F be a finite set of points in $\mathbb{R}^s$. Suppose that there are real scalars $z_{i\ell}$ $(1 \leqslant i \leqslant s, \ell \in \mathbb{N})$, a positive integer m, and a linear automorphism $\sigma \in \mathrm{GL}(\mathbb{R}^s)$ such that $z_{ik} \neq z_{i\ell}$ whenever $k \neq \ell$, and that*

$$\sigma(F) \subset \{(z_{1\alpha_1}, z_{2\alpha_2}, \ldots, z_{s\alpha_s}) \in \mathbb{R}^s : \alpha \in \mathbb{N}^s,\ |\alpha| \leqslant m\}. \tag{9}$$

Then $\mu(F) \leqslant m$.

[1]This term is meant as only provisional; cf. [34].

References

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, J. Combin. Theory 6 (1969) 122–151.

[2] C. Bachoc, On harmonic weight enumerators of binary codes, Des. Codes Cryptogr. 18 (1999) 11–28.

[3] E. Bannai, E. Bannai, S. Suda, and H. Tanaka, On relative t-designs in polynomial association schemes, Electron. J. Combin. 22 (2015) #P4.47; arXiv:1303.7163.

[4] E. Bannai and T. Ito, Algebraic combinatorics I: Association schemes, Benjamin/Cummings, Menlo Park, CA, 1984.

[5] E. Bannai, M. Koike, M. Shinohara, and M. Tagami, Spherical designs attached to extremal lattices and the modulo p property of Fourier coefficients of extremal modular forms, Mosc. Math. J. 6 (2006) 225–264.

[6] A. Bonnecaze, E. Rains, and P. Solé, 3-colored 5-designs and $\mathbf{Z}_4$-codes, J. Statist. Plann. Inference 86 (2000) 349–368.

[7] C. de Boor and A. Ron, On multivariate polynomial interpolation, Constr. Approx. 6 (1990) 287–302.

[8] C. de Boor and A. Ron, The least solution for the polynomial interpolation problem, Math. Z. 210 (1992) 347–378.

[9] A. E. Brouwer, A. M. Cohen, and A. Neumaier, Distance-regular graphs, Springer-Verlag, Berlin, 1989.

[10] A. R. Calderbank and P. Delsarte, On error-correcting codes and invariant linear forms, SIAM J. Discrete Math. 6 (1993) 1–23.

[11] A. R. Calderbank, P. Delsarte, and N. J. A. Sloane, A strengthening of the Assmus–Mattson theorem, IEEE Trans. Inform. Theory 37 (1991) 1261–1268.

[12] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl. No. 10 (1973).

[13] P. Delsarte and V. I. Levenshtein, Association schemes and coding theory, IEEE Trans. Inform. Theory 44 (1998) 2477–2504.

[14] M. Gasca and T. Sauer, Polynomial interpolation in several variables, Adv. Comput. Math. 12 (2000) 377–410.

[15] D. Gijswijt, A. Schrijver, and H. Tanaka, New upper bounds for nonbinary codes based on the Terwilliger algebra and semidefinite programming, J. Combin. Theory Ser. A 113 (2006) 1719–1731.

[16] C. D. Godsil, Generalized Hamming schemes, manuscript (2010); arXiv:1011.1044.

[17] T. A. Gulliver and M. Harada, Extremal double circulant type II codes over $\mathbb{Z}_4$ and construction of 5-$(24, 10, 36)$ designs, Discrete Math. 194 (1999) 129–137.

[18] M. Harada, New 5-designs constructed from the lifted Golay code over $\mathbb{Z}_4$, J. Combin. Des. 6 (1998) 225–229.

[19] T. Helleseth, C. Rong, and K. Yang, On t-designs from codes over $\mathbf{Z}_4$, Discrete Math. 238 (2001) 67–80.

[20] G. Höhn, Self-dual codes over the Kleinian four group, Math. Ann. 327 (2003) 227–255; arXiv:math/0005266.

[21] P. Iliev, A Lie-theoretic interpretation of multivariate hypergeometric polynomials, Compos. Math. 148 (2012) 991–1002; arXiv:1101.1683.

[22] P. Iliev and P. Terwilliger, The Rahman polynomials and the Lie algebra $\mathfrak{sl}_3(\mathbb{C})$, Trans. Amer. Math. Soc. 364 (2012) 4225–4238; arXiv:1006.5062.

[23] J.-L. Kim and V. Pless, Designs in additive codes over $GF(4)$, Des. Codes Cryptogr. 30 (2003) 187–199.

[24] J. Lahtonen, K. Ranto, and R. Vehkalahti, 3-designs from all $\mathbf{Z}_4$-Goethals-like codes with block size 7 and 8, Finite Fields Appl. 13 (2007) 815–827.

[25] W. J. Martin and H. Tanaka, Commutative association schemes, European J. Combin. 30 (2009) 1497–1525; arXiv:0811.2475.

[26] T. Miezaki and H. Nakasora, An upper bound of the value of t of the support t-designs of extremal binary doubly even self-dual codes, Des. Codes Cryptogr. 79 (2016) 37–46; arXiv:1311.2122.

[27] H. Mizukawa and H. Tanaka, $(n+1, m+1)$-hypergeometric functions associated to character algebras, Proc. Amer. Math. Soc. 132 (2004) 2613–2618.

[28] J. V. S. Morales, On Lee association schemes over $\mathbb{Z}_4$ and their Terwilliger algebra, Linear Algebra Appl. 510 (2016) 311–328.

[29] J. V. S. Morales and H. Tanaka, An Assmus-Mattson Theorem for Codes over Commutative Association Schemes, submitted to Designs Codes Cryptogr.; arXiv:1610.07334.

[30] A. Schrijver, New code upper bounds from the Terwilliger algebra and semidefinite programming, IEEE Trans. Inform. Theory 51 (2005) 2859–2866.

[31] D.-J. Shin, P. V. Kumar, and T. Helleseth, An Assmus–Mattson-type approach for identifying 3-designs from linear codes over $\mathbf{Z}_4$, Des. Codes Cryptogr. 31 (2004) 75–92.

[32] J. Simonis, MacWilliams identities and coordinate partitions, Linear Algebra Appl. 216 (1995) 81–91.

[33] P. Solé, The Lee association scheme, in: G. Cohen and P. Godlewski (eds.), Coding theory and applications, Lecture Notes in Computer Science, vol. 311, Springer-Verlag, Berlin, 1988, pp. 45–55.

[34] J. N. Srivastava and D. V. Chopra, Balanced arrays and orthogonal arrays, in: J. N. Srivastava (ed.), A survey of combinatorial theory, North-Holland, Amsterdam, 1973, pp. 411–428.

[35] K. Tanabe, An Assmus–Mattson theorem for $\mathbf{Z}_4$-codes, IEEE Trans. Inform. Theory 46 (2000) 48–53.

[36] K. Tanabe, A new proof of the Assmus–Mattson theorem for non-binary codes, Des. Codes Cryptogr. 22 (2001) 149–155.

[37] K. Tanabe, A criterion for designs in $\mathbb{Z}_4$-codes on the symmetrized weight enumerator, Des. Codes Cryptogr. 30 (2003) 169–185.

[38] H. Tanaka, New proofs of the Assmus–Mattson theorem based on the Terwilliger algebra, European J. Combin. 30 (2009) 736–746; arXiv:math/0612740.

[39] H. Tanaka, R. Tanaka, and Y. Watanabe, The Terwilliger algebra of a Q-polynomial distance-regular graph with respect to a set of vertices, in preparation.

[40] H. Tarnanen, On extensions of association schemes, in: H. Laakso and A. Salomaa (eds.), The very knowledge of coding, University of Turku, Institute for Applied Mathematics, Turku, 1987, pp. 128–142.

[41] P. Terwilliger, The subconstituent algebra of an association scheme I, J. Algebraic Combin. 1 (1992) 363–388.

[42] P. Terwilliger, The subconstituent algebra of an association scheme II, J. Algebraic Combin. 2 (1993) 73–103.

[43] P. Terwilliger, The subconstituent algebra of an association scheme III, J. Algebraic Combin. 2 (1993) 177–210.

[44] P. Terwilliger, The displacement and split decompositions for a Q-polynomial distance-regular graph, Graphs Combin. 21 (2005) 263–276; arXiv:math.CO/0306142.

[45] P. Terwilliger, Six lectures on distance-regular graphs, lecture notes, De La Salle University, 2010; `http://www.math.wisc.edu/~terwilli/teaching.html` .